

R 221400Z SEP 03 CNO WASHINGTON DC

TO COMLANTFLT NORFOLK VA  
COMUSNAVEUR LONDON UK  
COMPACFLT PEARL HARBOR HI  
OPNAVSUPACT WASHINGTON DC  
FLDSUPACT WASHINGTON DC  
COMUSNAVCENT  
COMNAVRESFOR NEW ORLEANS LA  
NETC PENSACOLA FL  
BUMED WASHINGTON DC  
COMNAVSEASYS COM WASHINGTON DC  
CHNAVPERS MEMPHIS TN  
COMSC WASHINGTON DC  
USNA ANNAPOLIS MD  
COMNAVSUPSYSCOM MECHANICSBURG PA  
NAVWARCOL NEWPORT RI  
COMNAVLEGSVCCOM WASHINGTON DC  
COMSPAWARSYSCOM SAN DIEGO CA  
NAVPGSCOL MONTEREY CA  
COMNAVFACENGCOM WASHINGTON DC  
NAVSTKAIRWARCEN FALLON NV  
COMNAVSECGRU FORT GEORGE G MEADE MD  
DIRSSP WASHINGTON DC  
COMNAVAIRESYSCOM PATUXENT RIVER MD  
PRESINSURV NORFOLK VA  
ONI WASHINGTON DC  
COMNAVSAFECEN NORFOLK VA  
NAVOBSY WASHINGTON DC  
COMNAVMETOCCOM STENNIS SPACE CENTER MS  
COMNAVDIST WASHINGTON DC  
COMNAVSPECWARCOM CORONADO CA  
NAVHISTCEN WASHINGTON DC  
NCTSI SAN DIEGO CA  
PEO IT WASHINGTON DC

INFO USJFCOM NORFOLK VA  
USPACOM HONOLULU HI  
DON CIO WASHINGTON DC  
CMC WASHINGTON DC  
CMC WASHINGTON DC  
COMFLTFORCOM NORFOLK VA

COMNAVNETWARCOM NORFOLK VA  
PEO C4I AND SPACE SAN DIEGO CA  
COMDT COGARD WASHINGTON DC  
COMOPTEVFOR NORFOLK VA

ADMINISTRATIVE MESSAGE

ROUTINE

UNCLAS

MSGID/GENADMIN/CNO WASHINGTON DC/N614/-/SEP//

SUBJ/DOD PUBLIC KEY INFRASTRUCTURE (PKI) AMPLIFYING IMPLEMENTATION  
/GUIDANCE//

REF/A/MSG/CNO/011600ZMAY2003//

REF/B/DOC/ASSTSECDEF WASH DC/21MAY2002//

REF/C/MSG/DON CIO WASH DC/151407ZSEP2003/-/PASEP//

REF/D/DOC/DON CIO WASH DC/19MAY2003//

REF/E/DOC/DOD WASH DC/24OCT2002//

NARR/REF A IS CNO PKI IMPLEMENTATION GUIDANCE. REF B PROMULGATED THE DOD  
PKI POLICY AND MILESTONES UPDATE. REF C IS THE DON CIO MSG AUTHORIZING A  
SIX MONTH EXTENSION FOR DON COMPLIANCE WITH THE DOD MANDATES. REF D IS  
DON CIO SMART CARD AND PKI POLICY. REF E IS THE DOD INFORMATION  
ASSURANCE DIRECTIVE.// POC/MR. R. WEILMINSTER/CIV/OPNAV N61424/LOC:WASH  
DC  
/TEL:(703) 601-1296/TEL:DSN: 329-1296  
/EMAIL:ROBERT.WEILMINSTER1(AT)NAVY.MIL//

RMKS/1. THIS IS A PROGRAM EXECUTIVE OFFICE-COMMAND, CONTROL,  
COMMUNICATIONS, COMPUTERS AND INTELLIGENCE AND SPACE (PEO C4I AND  
SPACE) (PMW 161), COMNAVNETWARCOM (N64), CNO (N614) AND DON CIO  
COORDINATED MESSAGE TO PROVIDE AMPLIFYING IMPLEMENTATION GUIDANCE TO  
REF  
A AND ESTABLISH COMPLIANCE REPORTING REQUIREMENTS.

2. A DETAILED NAVY PKI IMPLEMENTATION POA&M HAS BEEN DEVELOPED BY PEO C4I AND SPACE (PMW 161) IN COORDINATION WITH NETWARCOM (N64). THE PLAN, WHICH ADDRESSES NMCI, OCONUS, AFLOAT, AND NON-NMCI CONUS ENVIRONMENTS, INDICATES THAT FULL IMPLEMENTATION WITHIN NAVY WILL LIKELY NOT BE ACHIEVED UNTIL 1ST QTR CY04. AS A RESULT, DON CIO HAS AUTHORIZED A SIX MONTH EXTENSION UNTIL 1 APRIL 2004 FOR COMPLIANCE WITH THE DOD PKI MILESTONES OF REF B AND HAS CONCURRED WITH THE NAVY DEPLOYMENT AND IMPLEMENTATION GUIDANCE AS DETAILED BELOW. NAVY PLANS TO DEPLOY AND IMPLEMENT PKI AS QUICKLY AS POSSIBLE, BUT NO LATER THAN 1 APRIL 2004 AND REQUIRE MONTHLY REPORTING ON PROGRESS TOWARD FULL COMPLIANCE.

3. SPECIFIC GUIDANCE FOR NAVY PKI DEPLOYMENT AND IMPLEMENTATION: A. WEB SITES: ALL NAVY UNCLASSIFIED PRIVATE WEB SITES SHOULD ALREADY BE PUBLIC KEY ENABLED FOR SERVER-SIDE CERTIFICATE-BASED AUTHENTICATION USING DOD PKI SERVER CERTIFICATES AND SECURE SOCKETS LAYER (SSL) SESSION ENCRYPTION. ANY SITE NOT YET COMPLIANT SHALL TAKE IMMEDIATE ACTION TO ENSURE COMPLIANCE NLT 15 OCT 2003. NLT 1 NOV 2003 WEB SITES SHALL BEGIN TO POST A BANNER INDICATING THAT THEY ARE A DOD PRIVATE WEB SITE AND WILL IMPLEMENT CLIENT-SIDE STRONG AUTHENTICATION USING DOD PKI CERTIFICATES NLT 1 APRIL 2004. IN THE MEANTIME, IF FEASIBLE, IMPLEMENT A DUAL AUTHENTICATION APPROACH (I.E., ACCESSING WITH AND WITHOUT USERS' PKI CERTIFICATE) TO ALLOW PK ENABLED USERS THE OPPORTUNITY TO USE THEIR CERTIFICATES PRIOR TO THE 1 APRIL MANDATORY IMPLEMENTATION DATE. WEB SITES (E.G., NAVY KNOWLEDGE ONLINE) WHICH SUPPORT USERS WHO WILL NOT BE ISSUED PKI CERTIFICATES (I.E., DEPENDENTS, RETIREES, IRR) MAY CONTINUE THE USE OF THE DUAL AUTHENTICATION APPROACH BEYOND 1 APRIL 2004. B. CERTIFICATES: THE NAVY EBUSINESS OPERATIONS OFFICE IS MANAGING ISSUANCE OF THE CAC TO DON PERSONNEL. [EACH USER IN THE TARGETED POPULATION (ACTIVE DUTY MILITARY, SEL RESERVE, DOD CIVIL SERVANTS, AND ELIGIBLE CONTRACTORS) SHOULD OBTAIN A CAC AS SOON AS POSSIBLE.] PLEASE ADVISE THAT THEY MUST ENSURE THEIR CORRECT EMAIL ADDRESS AND THE ASSOCIATED CERTIFICATES ARE ENCODED TO THEIR CAC AT THE TIME OF ISSUANCE, AND BE SURE TO SELECT A 6-8 DIGIT NUMERIC PERSONAL IDENTIFICATION NUMBER (PIN) WHICH THEY WILL REMEMBER. COMMANDS SHOULD KEEP ISSUANCE OF SOFTWARE CERTIFICATES, OUTSIDE OF THE AFLOAT ENVIRONMENT, TO A MINIMUM AND ISSUED THEM ONLY WHEN OPERATIONALLY NECESSARY (E.G., ACCESS TO OUTLOOK WEB ACCESS (OWA)). C. E-MAIL SIGNING: MESSAGES CONTAINING MISSION ASSURANCE CATEGORY 1 (MAC 1) (FORMALLY MISSION CRITICAL) AND/OR MAC 2 (FORMALLY MISSION SUPPORT) INFORMATION SHALL BE DIGITALLY SIGNED. ALSO, DIGITALLY SIGN ALL EMAIL REQUIRING EITHER MESSAGE INTEGRITY AND/OR NON-REPUDIATION. E-MAIL SYSTEMS WHICH ARE USED SOLELY FOR PERSONAL, NON OFFICIAL MAIL (E.G., SAILOR MAIL) DO NOT NEED TO IMPLEMENT DIGITAL SIGNING. D. E-MAIL

ENCRYPTION: ENCRYPT MESSAGES CONTAINING SENSITIVE INFORMATION AS DEFINED IN REF E ENCLOSURE 2 (PARA E2.1.41). OBTAIN PUBLIC KEY ENCRYPTION CERTIFICATES BY RECEIVING A SIGNED EMAIL FROM THE INTENDED RECIPIENT OR BY DOWNLOADING INDIVIDUAL CERTIFICATES FROM THE GLOBAL DIRECTORY SERVICE

AT HTTPS:(SLANT/SLANT)DOD411.CHAMB.DISA.MIL/

E. CRYPTOGRAPHIC BASED NETWORK LOGON: DOD IS IMPLEMENTING CRYPTOGRAPHIC (I.E., CERTIFICATE) BASED LOGON (USING THE CAC) AS THE STANDARD MECHANISM FOR ACCESS TO DOD NETWORKS. NMCI IS DEPLOYING THE INFRASTRUCTURE COMPONENTS REQUIRED TO SUPPORT THIS CAPABILITY. NAVY PROJECTS COMPLETION OF THE POA&M FOR ALL NON-NMCI NAVY SEATS BY THE END OF SEP 2003.

4. THE NAVY IS COMMITTED TO MOVING FORWARD AS QUICKLY AS POSSIBLE TO FULLY IMPLEMENT NETWORK SECURITY USING PUBLIC KEY TECHNOLOGY IN ALL LOCATIONS AND OPERATING ENVIRONMENTS. TO PROVIDE THE CAPABILITY TO POSITIVELY MEASURE PROGRESS TOWARD THIS GOAL, ALL SECOND ECHELON COMMANDS WILL PROVIDE THE FOLLOWING: A. PROVIDE CONTACT INFORMATION FOR COMMAND'S SMART CARD TECHNOLOGY POC PER REF D. SUBMISSIONS ARE DUE TO ROBERT WEILMINSTER (CNO

(N6142)) AT ROBERT.WEILMINSTER1(AT)NAVY.MIL NLT 15 OCT 2003.

B. PROVIDE CONTACT INFORMATION FOR COMMAND'S PKI POC (CAN BE THE SAME INDIVIDUAL AS ABOVE). SUBMISSIONS ARE DUE TO CNO (N6142). NLT 15 OCT 2003. C. PROVIDE INITIAL PKI IMPLEMENTATION STATUS REPORT THROUGH THE END OF OCT 2003 FOR ALL COMMANDS WITHIN YOUR CLAIMANCY TO PEO C4I AND SPACE (PMW 161-2A) MR. SAMIR OTHMAN AT SAMIR.OTHMAN(AT)NAVY.MIL NLT 10 NOV 2003. FORMAT FOR THIS STATUS REPORT SUBMISSION IS AVAILABLE AT (URL IS ALL UPPER CASE)

HTTPS:(SLANT/.SLANT)INFOSEC.NAVY.MIL/PKI/ECH2\_PKICOMPLIANCEREPORT.

MONTHLY FOLLOW-ON PKI STATUS REPORT SUBMISSIONS ARE DUE TO SAMIR OTHMAN (PMW 161-2A) ON 01 DEC, 01 JAN, 01 FEB, 01 MAR AND 01 APR. ONCE 100 PERCENT IMPLEMENTATION IS ACHIEVED, REPORTS ARE NO LONGER REQUIRED.

5. ADDRESS IMPLEMENTATION QUESTIONS AND REQUESTS FOR SUPPORT TO PEO C4I AND SPACE (PMW 161-2A) MR. SAMIR OTHMAN AT SAMIR.OTHMAN(AT)NAVY.MIL. ADDRESS POLICY QUESTIONS TO CNO (N614) MR. ROBERT WEILMINSTER AT ROBERT.WEILMINSTER1(AT)NAVY.MIL.

6. WIDEST DISSEMINATION REQUESTED.//

BT

#0655

NNNN

RTD:000-000/COPIES: